Galois Theory

Swayam Chube

Last Updated: May 6, 2025

Contents

§1 Algebraic Extensions

§§ Algebraic Elements

Definition 1.1. A *field extension* is a containment of fields $F \subseteq E$. The dimension of E when viewed as a vector space over F is called the *degree* of the extension and is denoted $[E : F]$.

An element $\alpha \in E$ is said to be *algebraic* over F if it satisfies an equation of the form

$$a_n \alpha^n + \cdots + a_0 = 0,$$

where not all the a_i's are zero. An element of E which is not algebraic is said to be transcendental over F. The extension $F \subseteq E$ is said to be *algebraic* if every element of E is algebraic over F.

Let $\alpha \in E$ be algebraic over F as in the above definition. Consider the ring homomorphism $\varphi : F[X] \to E$ which is identity on F and sends $X \mapsto \alpha$. Clearly the kernel of this homomorphism is non-zero since it contains the non-zero polynomial $a_n X^n + \cdots + a_0$. Further, the image, being a subring of E is an integral domain, whence the kernel is a prime ideal. Since $F[X]$ is a PID, every prime ideal is maximal and is generated by an irreducible polynomial. Further, since $(F[X])^\times = F^\times$, there is a unique monic (irreducible) polynomial $p(X)$ such that $\ker \varphi = (p(X))$. This is called *the minimal polynomial* of α over F, denoted by $\mathrm{Irr}(\alpha, F, X)$. The image of φ is clearly $F[\alpha]$ and since we have argued that it is a field, we have shown that $F[\alpha] = F(\alpha)$. To summarize:

Proposition 1.2. Let $F \subseteq E$ be a field extension and $\alpha \in E$ be algebraic over F with minimal polynomial $p(X) \in F[X]$. Then $F[\alpha] = F(\alpha)$, and $[F(\alpha) : F] = \deg p(X)$. In particular, $F \subseteq F(\alpha)$ is a finite extension.

PROPOSITION 1.3. If $[E:F] < \infty$, then $F \subseteq E$ is algebraic.

Proof. Let $n = [E:F]$ and $\alpha \in E$. Thus the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent whence the conclusion follows. ■

PROPOSITION 1.4. Let $k \subseteq F \subseteq E$ be a tower of finite extensions. Then

$$[E:k] = [E:F][F:k].$$

Proof. Let $\{x_i\}$ be a k-basis for F and $\{y_j\}$ an F-basis for E. It is straightforward to check that $\{x_i y_j\}$ is a k-basis for E. ■

COROLLARY 1.5. A finitely generated algebraic extension is finite.

Proof. Let $F \subseteq E$ be a finitely generated algebraic extension, that is, there exist $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$. Considering the tower of field extensions:

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_n) = E,$$

and using Proposition 1.2 and Proposition 1.4, the conclusion follows. ■

DEFINITION 1.6. A class $\mathscr{C}$ of field extensions is said to form a *distinguished class* if the following two conditions are satisfied:

(DC 1) if $k \subseteq F \subseteq E$, then E/k is an element of $\mathscr{C}$ if and only if both E/F and F/k lie in $\mathscr{C}$.

(DC 2) if E/k is an element of $\mathscr{C}$ and F/k is any extension with both E and F contained in a larger ambient field, then EF/F lies in $\mathscr{C}$.

REMARK 1.7. It follows formally from (DC 1) and (DC 2) that if E/k and F/k lie in $\mathscr{C}$ with both E and F contained in a larger ambient field, then EF/k lies in $\mathscr{C}$.

THEOREM 1.8. Algebraic extensions form a distinguished class.

Proof. Let $k \subseteq F \subseteq E$ be a tower of extensions. Clearly if E/k is algebraic, then both E/F and F/k are algebraic from the definition. Suppose now that both E/F and F/k are algebraic and let $\alpha \in E$. Then α satisfies an algebraic equation over F:

$$a_n \alpha^n + \cdots + a_0 = 0,$$

where not all the a_i's are zero. Consider the tower of fields:

$$k \subseteq k(a_0, \ldots, a_n) = K \subseteq K(\alpha).$$

Note that α is algebraic over K, and hence both K/k and $K(\alpha)/K$ are finite due to Corollary 1.5 and Proposition 1.2 respectively. It follows from Proposition 1.4 that $K(\alpha)/k$ is finite, and hence algebraic due to Proposition 1.3. This verifies (DC 1).

Next, let $k \subseteq E$ be algebraic and $k \subseteq F$ be arbitrary with both E and F contained in a larger ambient field. Note that every $\alpha \in EF = F(E)$ is contained in a finitely generated subextension $F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. Since each α_i is algebraic over k and $k \subseteq F$, the extension $F \subseteq F(\alpha_1, \ldots, \alpha_n)$ is algebraic due to Corollary 1.5, and hence α is algebraic over F. This verifies (DC 2), thereby completing the proof. ■

§§ Algebraic Closure

DEFINITION 1.9. A field Ω is said to be *algebraically closed* if every non-constant polynomial in $\Omega[X]$ has a root in Ω.

LEMMA 1.10. Let k be a field and $p(X) \in k[X]$ a non-constant polynomial. Then there is an extension $k \subseteq E$ in which $p(X)$ has a root.

Proof. Without loss of generality, we may assume that $p(X)$ is irreducible. Consider the embedding of fields $k \hookrightarrow k[X]/p(X)$. We may identify k with its image under the above embedding. Clearly $\overline{X} \in k[X]/p(X)$ is a root of $p(X)$, thereby completing the proof. ∎

Corollary 1.11. Inductively, it is clear that given any finite collection of polynomials $f_1(X), \ldots, f_n(X) \in k[X]$, there exists an extension $k \subseteq E$ in which each of them have a root.

Theorem 1.12 (Artin). Every field is contained in an algebraically closed field.

Proof. Let k be a field. Set $K_0 = k$. For each non-constant polynomial $f \in k[X]$, introduce a new variable X_f, and let $R = k[\{X_f\}]$ be a polynomial ring over those infinite variables. Let $I \trianglelefteq R$ denote the ideal generated as

$$I \coloneqq \big(f(X_f) \colon f \in k[X] \text{ is a non-constant polynomial}\big).$$

We contend that I is a proper ideal. Suppose not, then there exist $g_1, \ldots, g_n \in R$ and non-constant polynomials $f_1, \ldots, f_n \in k[X]$

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

in R. Let F be an extension of k in which each f_i has a root for $1 \leqslant i \leqslant n$. Pick a root $\alpha_i \in F$ for each f_i. Substituting $X_{f_i} \mapsto \alpha_i$, we obtain an immediate contradiction. Thus I is a proper ideal, whence is contained in a maximal ideal $\mathfrak{m}$ of R. Set $K_1 = R/\mathfrak{m}$. Clearly $K_0 \subseteq K_1$ and every non-constant polynomial in $K_0[X]$ has a root in K_1. Similarly construct $K_1 \subseteq K_2 \subseteq \ldots$ and set $K \coloneqq \bigcup_{i=0}^{\infty} K_i$.

We contend that K is algebraically closed. Indeed, let $f(X) = a_n X^n + \cdots + a_0$ be a non-constant polynomial. Then, there is a sufficiently large $N \gg 0$ with $a_i \in K_N$ for all $0 \leqslant i \leqslant n$. Then, by construction, $f(X)$ has a root in $K_{N+1} \subseteq K$, thereby completing the proof. ∎

Remark 1.13. In [Lan02, Chapter VI, Exercise 28], one shows that K_1 itself is algebraically closed.

Corollary 1.14. Let k be a field. Then there exists an algebraic extension $k \subseteq k^a$ where k^a is algebraically closed.

Proof. Let Ω be an algebraically closed field containing k and set

$$k^a = \{\alpha \in \Omega \colon \alpha \text{ is algebraic over } k\}.$$

To see that k^a forms a field, note that if $\alpha, \beta \in k^a$, with $\alpha, \beta \neq 0$, then $k \subseteq k(\alpha, \beta)$ is an algebraic extension due to Corollary 1.5. In particular, $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1} \in k(\alpha, \beta)$ are algebraic over k and hence lie in k^a. Thus k^a is a field.

Let $f(X) \in k^a[X]$ be a non-constant polynomial. Since Ω is algebraically closed, $f(X)$ has a root $\alpha \in \Omega$ and α is algebraic over k^a, therefore is algebraic over k due to Theorem 1.8. In particular, $\alpha \in k^a$ and hence k^a is algebraically closed. ∎

Remark 1.15. Using an analogous proof, one can show that given any extension of fields $k \subseteq E$, the subset

$$E^a \coloneqq \{\alpha \in E \colon \alpha \text{ is algebraic over } k\}$$

is a field containing k and is algebraic over k.

Definition 1.16. Let $k \subseteq F$ and $k \subseteq E$ be field extensions. A *k-embedding* $\sigma \colon F \to E$ is a field homomorphism which restricts to the identity map on k.

Next we examine extensions of field embeddings. Let k be a field and $\sigma \colon k \to \Omega$ be an embedding into an algebraically closed field Ω. Let $k(\alpha) \supseteq k$ be an algebraic extension. Let $p(X) \in k[X]$ be the minimal polynomial of α over k. For any root $\beta \in \Omega$ of p^σ, it is clear from the isomorphism $k(\alpha) \cong k[X]/p(X)$ that the embedding σ can be extended to an embedding $\widetilde{\sigma} \colon k(\alpha) \to \Omega$ sending $\alpha \mapsto \beta$. Conversely, it is also clear that any such embedding must send α to a root of p^σ in Ω. In particular, we have:

Lemma 1.17. The number of extensions of σ to $k(\alpha)$ is equal to the number of distinct roots of $p^\sigma(X)$ in Ω.

Lemma 1.18 (Extension Lemma). Let E/k be an algebraic extension and Ω an algebraically closed field. Any embedding $\sigma : k \to \Omega$ can be extended to an embedding $E \to \Omega$.

Proof. This is a standard application of Zorn's lemma. We only sketch the proof. Let

$$\Sigma = \{(F, \sigma_F) : k \subseteq F \subseteq E,\ \sigma_F \text{ is an embedding of } F \text{ into } \Omega \text{ extending } \sigma\}.$$

Clearly Σ is a poset containing a maximal element, say (M, σ_M). If $M \neq E$, then choose some $\alpha \in E \setminus M$ and using Lemma 1.17, derive a contradiction. ∎

Corollary 1.19. Let k be a field with algebraic extensions $k \subseteq E$ and $k \subseteq E'$ where both E and E' are algebraically closed. Then there is a k-isomorphism $\tau : E \to E'$.

Proof. The inclusion $k \hookrightarrow E$ extends to a k-embedding $\tau : E \to E'$. Clearly $\tau(E)$ is an algebraically closed subfield of E' and hence must be equal to E'. ∎

Definition 1.20. Let k be a field. An algebraically closed field $k^a \supseteq k$ which is algebraic over k is said to be an *algebraic closure* of k. Due to Corollary 1.19, the algebraic closure is unique up to isomorphism.

Proposition 1.21. Let E/k be an algebraic extension and $\sigma : E \to E$ be a k-embedding (i.e., $\sigma|_k = \mathbf{id}_k$). Then σ is an automorphism of E.

Proof. It suffices to show that σ is surjective. Indeed, let $\alpha \in E$ and $p(X) \in k[X]$ denote the minimal polynoial of α over k. Since the coefficients of p are invariant under the action of the embedding, σ must send a root of p to another root of p. Further, since σ is injective and there are only finitely many roots of p in E, σ permutes the roots of p. In particular, there is some root β of p in E such that $\sigma\beta = \alpha$, whence surjectivity follows. ∎

§§ Splitting Fields and Normal Extensions

§§ Separable Extensions

§§ Finite Fields

§§ Purely Inseparable Extensions

§2 Galois Theory

§§ The Fundamental Theorem

§§ Cyclotomic Extensions

§§ Norm and Trace

§§ Hilbert's Theorem 90 and Applications

Theorem 2.1 (Hilbert's Theorem 90, Multiplicative Form). Let K/k be a cyclic Galois extension of degree n with Galois group G. Let σ be a generator of G and $\beta \in K$. Then $N_k^K(\beta) = 1$ if and only if there exists an element $\alpha \neq 0$ in K such that $\beta = \alpha/\sigma\alpha$.

Proposition 2.2. Let k be a field and n be a positive integer prime to the characteristic of k, and assume that there is a primitive n-th root of unity in k.

(1) Let K/k be a cyclic extension of degree n. Then there exists an $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in k$.

(2) Conversely, let $a \in k$ and let α be a root of $X^n - a$. Then $k(\alpha)/k$ is cyclic of degree $d \mid n$, and $\alpha^d \in k$.

Theorem 2.3 (Hilbert's Theorem 90, Additive Form). Let k be a field and K/k a cyclic extension of degree n with Galois group G. Let σ be a generator of G and $\beta \in K$. Then $\mathrm{Tr}_k^K(\beta) = 0$ if and only if there exists an element $\alpha \in K$ such that $\beta = \alpha - \sigma\alpha$.

THEOREM 2.4 (ARTIN-SCHREIER). Let k be a field of characteristic $p > 0$.

(1) Let K/k be a cyclic extension of degree p. Then there exists an $\alpha \in K$ such that $K = k(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ for some $a \in k$.

(2) Conversely, given $a \in k$, the polynomial $f(X) = X^p - X - a$ either has one root in k, in which case, all its roots are in k, or it is irreducible. In the latter case, if α is a root, then $k(\alpha)/k$ is a cyclic extension of degree p.

§§ The Artin-Schreier Theorem

DEFINITION 2.5. A field F is said to be *formally real* if -1 cannot be written as a sum of squares in F. It is said to be *real closed* if it is formally real and does not admit a proper formally real algebraic extension.

REMARK 2.6. First, note that any formally real field must be characteristic 0, because we can write

$$-1 = \underbrace{1 + 1 + \cdots + 1}_{p-1 \text{ times}}$$

in a field of characteristic $p > 0$.

A standard argument using Zorn's lemma shows that every formally real field is contained in a real closed field which is algebraic over it. Further, it is an easy consequence of [Lan02, Chapter V, Exercise 28] that an odd degree extension of a formally real field is formally real.

THEOREM 2.7 (ARTIN-SCHREIER). Let $F \subseteq L$ be an extension of fields with L algebraically closed and $1 < [L : F] < \infty$. Then

(1) $[L : F] = 2$ and $L = F[\iota]$ where $\iota \in L$ and $\iota^2 = -1$.

(2) if S denotes the set of non-zero squares in F, then S is closed under addition.

(3) $F = S \sqcup \{0\} \sqcup -S$, where $-S = \{-s : s \in S\}$.

(4) F is real closed.

We shall deduce this theorem as a result of several lemmas.

LEMMA 2.8. Suppose $\operatorname{char} F = p > 0$ and F is not perfect. Then there exist irreducible polynomials of degree p^e in $F[X]$ for each integer $e \geqslant 0$.

Proof. Since F is not perfect, there exists some $a \in F \setminus F^p$. We contend that $X^{p^e} - a$ is irreducible for each $e \geqslant 0$. This is clear for $e = 0$, so assume $e \geqslant 1$. Let $\alpha \in F^a$ denote the unique root of $X^{p^e} - a$. If $f(X) \in F[X]$ denotes the irreducible polynomial of α over F, then $X^{p^e} - a = f(X)^m$ for some positive integer m. Comparing degrees, it is clear that m is a prime power. If $m > 1$, then $p \mid m$, whence looking at constant terms, $a \in F^p$, a contradiction. ∎

In particular, this shows that under the hypothesis of Theorem 2.7, F must be perfect.

LEMMA 2.9. Under the hypothesis of Theorem 2.7. Then either $[L : F] = 2$ and $L = F[\iota]$ where $\iota^2 = -1$, or there exists an intermediate field $F \subseteq K \subseteq L$ such that

(i) L/K is Galois,

(ii) $[L : K] = p$ a prime, and

(iii) -1 is a square in K.

Proof. As we remarked, F must be perfect. Hence, L/F is Galois. Let $\iota \in L$ be a root of $X^2 + 1 \in L[X]$. If $F[\iota] = L$, then we are done. Else suppose $F \subseteq F[\iota] \subsetneq L$. Let $G = \operatorname{Gal}(L/F[\iota])$. Since G is a non-trivial finite group, it is possible to choose a subgroup of G having prime order, say $\operatorname{Gal}(L/K)$. This completes the proof. ∎

LEMMA 2.10. Let $K \subseteq L$ be a field extension with L algebraically closed, and $[L:K] = p$ a prime. If $\operatorname{char} K \neq p$, then K contains a primitive p-th root of unity.

Proof. Since $\operatorname{char} K \neq p$, the polynomial $X^p - 1 \in K[X]$ is separable. Choose a root $1 \neq \zeta \in L$. Clearly ζ is a primitive p-th root of unity in L. Then $[K(\zeta):K] \leqslant p-1$. Since L/K admits no proper intermediate fields, we must have $K(\zeta) = K$, i.e., $\zeta \in K$. ∎

THEOREM 2.11. Let $K \subseteq E$ be a Galois extension of degree p a prime and K contains a primitive p-th root of unity. If $p = 2$, assume further that -1 is a square in K. Then there exists an $\alpha \in E$ such that the polynomial $X^p - \alpha \in E[X]$ is irreducible. In particular, E is not algebraically closed.

Proof. Due to Proposition 2.2, there exists an $\alpha \in E$ such that $E = K(\alpha)$ where $\alpha^p = a \in K$. We shall show that $X^p - \alpha \in E[X]$ is irreducible. Let $\zeta \in K$ be a primitive p-th root of unity. If $\beta \in E^a$ is a root of $X^p - \alpha$, then due to Proposition 2.2, $E(\beta)/E$ is cyclic of degree $d \mid p$ and hence $d \in \{1, p\}$. If $[E(\beta):E] = p$, then we are done. Suppose now that $E(\beta) = E$, i.e., $\beta \in E$. We shall derive a contradiction.

Let $\operatorname{Gal}(E/K) = \langle \sigma \rangle$. Note that $\beta^{p^2} = \alpha^p = a \in K$, so that $\sigma(\beta)^{p^2} = a = \beta^{p^2}$. Set $\delta = \sigma(\beta)/\beta$. Then $\delta^{p^2} = 1$, so that δ^p is a p-th root of unity. Set $\varepsilon = \sigma(\delta)/\delta$. Then $\varepsilon^p = \sigma(\delta^p)/\delta^p = 1$, since the p-th roots of unity are contained in the base field K. Thus ε is a p-th root of unity, in particular, $\varepsilon \in K$.

It is easy to show using induction on $i \geqslant 1$ that

$$\sigma^i(\beta) = \beta \delta^i \varepsilon^{\frac{i(i-1)}{2}}.$$

Hence

$$\beta = \sigma^p(\beta) = \beta \delta^p \varepsilon^{\frac{p(p-1)}{2}}.$$

Thus

$$\delta^p \varepsilon^{\frac{p(p-1)}{2}} = 1.$$

Now, if p is odd, then $\varepsilon^{\frac{p(p-1)}{2}} = 1$, therefore $\delta^p = 1$, i.e., δ is a p-th root of unity. So

$$\sigma(\alpha) = \sigma(\beta^p) = \sigma(\beta)^p = \delta^p \beta^p = \alpha \implies \alpha \in K,$$

a contradiction.

Next, if $p = 2$, then $\delta^2 \varepsilon = 1$ so $\delta^4 = \varepsilon^{-2} = 1$, and hence $\delta^2 = \pm 1$. And since -1 is a square in K, we have that $\delta \in K$. Consequently, $\varepsilon = \sigma(\delta)/\delta = 1$. It follows that $1 = \delta^2 \varepsilon = \delta^2$. Thus

$$\sigma(\alpha) = \sigma(\beta^2) = \sigma(\beta)^2 = \delta^2 \beta^2 = \alpha \implies \alpha \in K,$$

a contradiction again. This completes the proof. ∎

THEOREM 2.12. Let $K \subseteq E$ be a Galois extension of prime degree p where $\operatorname{char} K = p > 0$. Then there exists an $\alpha \in E$ such that $X^p - X - \alpha \in E[X]$ is irreducible. In particular, E is not algebraically closed.

Proof. Due to Theorem 2.4, thre exists some $\beta \in E$ such that $E = K(\beta)$ and the minimal polynomial of β over K is of the form $X^p - X - b$ for some $b \in K$. Set $\alpha = \beta^{p-1} b$. We shall show that the polynomial $X^p - X - \alpha \in E[X]$ is irreducible. To this end, due to Theorem 2.4, it suffices to show that this polynomial has no roots in E.

Suppose $\gamma \in E$ is a root. Then $\gamma = g(\beta)$ for some $g(X) \in K[X]$ with $\deg g \leqslant p-1$. Let $h(X) \in K[X]$ be such that $g(X)^p = h(X^p)$. Then

$$\alpha = b\beta^{p-1} = \gamma^p - \gamma = h(\beta^p) - g(\beta) = h(\beta + b) - g(\beta).$$

Since $1, \beta, \ldots, \beta^{p-1}$ are linearly independent over $K<$ we can equate the coefficients on both sides. Let a be the coefficient of X^{p-1} in $g(X)$, then a^p is the coefficient of X^{p-1} in $h(X)$. Thus $a^p - a = b$, which is absurd, since $X^p - X - b$ is irreducible. This completes the proof. ∎

Proof of Theorem 2.7. (1) If the conclusion fails, then due to Lemma 2.9 there is a prime $p > 0$ and a subfield $F \subseteq K \subseteq L$ such that L/K is Galois of degree p and -1 is a square in K. Due to Theorem 2.12, $\operatorname{char} F \neq p$. Hence, by Lemma 2.10, K contains a primitive p-th root of unity. Finally, in this case, due to Theorem 2.11 L is not algebraically closed, a contradiction. Thus $[L:F] = 2$ and $L = F[\iota]$ where $\iota^2 = -1$.

(2) Then $\mathrm{Gal}(L/F) = \{1, \tau\}$, where $\tau(\iota) = -\iota$. Let $r, s \in F$ be non-zero. Note that $r^2 + s^2 = 0$ would imply $(r/s)^2 = -1$, which is not possible. Thus, it suffices to show that $r^2 + s^2$ is a square in F. Indeed, $r + \iota s \in L$ and hence, $r + \iota s = (a + \iota b)^2$ for some $a, b \in F$. Applying τ, we get that $r - \iota s = (a - \iota b)^2$. Multiplying these two, we get

$$r^2 + s^2 = (r + \iota s)(r - \iota s) = (a^2 + b^2)^2.$$

Thus, a sum of squares in F is a square.

(3) By definition, $0 \notin S$. If $S \cap -S$ were non-empty, then $-r^2 = s^2 \neq 0$ for some non-zero elements $r, s \in F$. But then again, this would mean $(s/r)^2 = -1$ in F, a contradiction. Thus, the sets $S, \{0\}, -S$ are pairwise disjoint. Let $0 \neq r \in F$. Since r is a square in L, we can write

$$r = (a + \iota b)^2 = (a^2 - b^2) + 2ab\iota.$$

Thus $2ab = 0$, whence $a = 0$ or $b = 0$[1], in either case, $r \in S$ or $r \in -S$, which shows that $F = S \sqcup \{0\} \sqcup -S$.

(4) From (2) and (3) it is clear that F is formally real. Any proper algebraic extension of F in L must be L, which is not formally real, therefore, F is real closed. ■

§§ Cyclic Kummer Theory

§§ Abelian Kummer Theory

§3 Transcendental Extensions

References

[Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer-Verlag New York, Inc., 2002.

[1] We are implicitly using the fact that $\mathrm{char}\, F \neq 2$, for if $\mathrm{char}\, F = 2$, then $X^2 + 1$ would have the unique solution $X = 1$.